Amendments to the Claims

Claim 1 (currently amended): A computer-implemented method of provisioning an aggregated service in a computing network, comprising steps of:

obtaining credentials of a user who requests to access an aggregated service;

locating, in a network-accessible registry, a service description document specifying a provisioning interface for the aggregated service, the aggregated service comprising an aggregation of a plurality of sub-services and the provisioning interface specifying how to invoke identity functions of the aggregated service;

analyzing the obtained credentials by invoking one or more of the identity functions, according to the specification thereof in the provisioning interface, to determine whether the user is authenticated for~~, and/or is authorized for,~~ accessing the aggregated service; and

allowing the user to access the aggregated service only if the analyzing step ~~has a successful result~~ determines that the user is authenticated for accessing the aggregated service.

Claim 2 (previously presented): The computer-implemented method according to Claim 1, wherein an implementation of each of the identify functions of the aggregated service is provided by at least one of the sub-services.

Claim 3 (currently amended): The computer-implemented method according to Claim 1, wherein:

at least one of the sub-services has a local provisioning interface, the local provisioning interface specified in a corresponding service description document and comprising a specification of how to invoke one or more identity functions of the sub-service; and

the identity functions in the provisioning interface of the aggregated service are selected from the local provisioning interfaces; and further comprising the step of:

controlling access to each of the sub-services having the local provisioning interface, further comprising the steps of:

determining whether the user is authenticated for,~~ and/or authorized for,~~ accessing the sub-service by invoking at least one of the one or more identity functions of the sub-service, according to the specification thereof in the local provisioning interface; and

allowing the user to access the sub-service only if the determining step ~~has a successful result~~ determines that the user is authenticated for accessing the sub-service.

Claim 4 (previously presented): The computer-implemented method according to Claim 3, wherein:

the step of obtaining credentials of the user also obtains sub-service credentials for at least one of the sub-services having the local provisioning interface; and

the determining step uses the obtained sub-service credentials.

Claim 5 (currently amended): The computer-implemented method according to Claim 1, wherein:

one or more operations of at least one of the sub-services is access-protected;

the obtaining step further comprises obtaining, for at least one of the access-protected operations, operation-specific credentials of the user; and further comprising the step of:

controlling access to each of at least one of the access-protected operations, further comprising the steps of:

analyzing the obtained operation-specific credentials by invoking one of more of the identity functions, according to the specification thereof in the provisioning interface, to determine whether the user can access the access-protected operation; and

allowing the user to access the access-protected operation only if the step of analyzing the obtained operation-specific credentials ~~has a successful result~~ determines that the user can access the access-protected operation.

Claim 6 (canceled)

Claim 7 (previously presented): The computer-implemented method according to Claim 1, wherein identity information obtained by invoking one or more of the identity functions is programmatically relayed among at least two of the sub-services of the aggregated service.

Claim 8 (previously presented): The computer-implemented method according to Claim 7, wherein the programmatic relaying comprises sending a message which specifies the identity information in a header of the message and which specifies a service request in a body of the message.

Claim 9 (previously presented): The computer-implemented method according to Claim 8, wherein the message is a SOAP ("Simple Object Access Protocol") message.

Claim 10 (previously presented): The computer-implemented method according to Claim 1, wherein the service description document is specified in a markup language.

Claim 11 (previously presented): The computer-implemented method according to Claim 10, wherein the markup language is Web Services Description Language ("WSDL").

Claim 12 (previously presented): The computer-implemented method according to Claim 2, wherein the network-accessible registry is accessed using standardized messages.

Claim 13 (currently amended): A system for provisioning an aggregated service in a computing network, comprising:

means for defining a provisioning interface of the aggregated service;

means for specifying the provisioning interface in a service description document;

means for obtaining credentials of a user who requests to access an aggregated service;

means for locating, in a network-accessible registry, a service description document specifying a provisioning interface for the aggregated service, the aggregated service comprising an aggregation of a plurality of sub-services and the provisioning interface specifying how to invoke identity functions of the aggregated service;

means for analyzing the obtained credentials by invoking one or more of the identity functions, according to the specification thereof in the provisioning interface, to determine whether the user is authenticated for, and ~~and/or~~ is authorized for, accessing the aggregated service; and

means for allowing the user to access the aggregated service only if the means for analyzing ~~has a successful result~~ determines that the user is authenticated for, and is authorized for, accessing the aggregated service.

Claim 14 (currently amended): A computer program product for provisioning an aggregated service in a computing network, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code [[means]] for obtaining credentials of a user who requests to access an aggregated service;

computer-readable program code [[means]] for locating, in a network-accessible registry, a service description document specifying a provisioning interface for the aggregated service, the aggregated service comprising an aggregation of a plurality of sub-services and the provisioning interface specifying how to invoke identity functions of the aggregated service;

computer-readable program code [[means]] for analyzing the obtained credentials by invoking one or more of the identity functions, according to the specification thereof in the provisioning interface, to determine whether the user is authenticated for, or ~~and/or~~ is authorized for, accessing the aggregated service; and

computer-readable program code [[means]] for allowing the user to access the aggregated service only if the computer-readable program code [[means]] for analyzing ~~has a successful result~~ determines that the user is authenticated for, or is authorized for, accessing the aggregated service.

Claim 15 (previously presented): The method according to Claim 1, wherein an implementation of at least one of the sub-services is located dynamically, at run-time.

Claim 16 (previously presented): The method according to Claim 7, wherein the identity information is initially obtained as a result of the analyzing step.

Claim 17 (previously presented): The method according to Claim 7, wherein the identity information comprises an authentication token generated by one of the invoked identity functions.

Claim 18 (previously presented): The method according to Claim 1, wherein:

at least two of the sub-services each have associated therewith an identity system for access control thereto;

at least two of the associated identity systems are heterogeneous; and

at least one selected one of the identity functions of the aggregated service enables dynamically joining at least two of the heterogeneous identity systems.

Claim 19 (previously presented): The method according to Claim 18, wherein the at least one selected identity function, upon invocation, identifies the identity system that stores information pertaining to users of the sub-service with which that identity system is associated.

Claim 20 (previously presented): The method according to Claim 19, wherein the dynamic joining is enabled by relaying the identification of the identity system among the dynamically-joined identity systems.

Claim 21 (new): The method according to Claim 1, wherein:

the analyzing step further comprises determining whether the user is authorized for accessing the aggregated service, and

the allowing step further comprises allowing the user to access the aggregated service only if the analyzing step determines that the user is both authenticated for, and authorized for, accessing the aggregated service.